セキュリティ
ユーザ ガイド

改訂第 1 版：2008 年 8 月

初版：2007 年 6 月

製品番号：490721-291

製品についての注意事項

このユーザ ガイドでは、ほとんどのモデルに共通の機能について説明します。一部の機能は、お使いのコンピュータで対応していない場合もあります。

目次

1 コンピュータの保護

注記： セキュリティ機能は、誤った取り扱いに対処することを目的としていますが、コンピュータの盗難や誤った取り扱いを完全に防ぐものではありません。

注記： お使いのコンピュータでは、オンライン セキュリティ ベースの追跡および復元サービスである[CompuTrace]がサポートされています（一部の地域のみ）。コンピュータが盗まれた場合、不正なユーザがインターネットにアクセスすると、[CompuTrace]による追跡が行われます。[CompuTrace]を使用するには、ソフトウェアを購入し、サービス登録を行う必要があります。[CompuTrace]ソフトウェアの購入については、HP Web サイト http://www.hpshopping.com/（英語サイト）にアクセスしてください。

お使いのコンピュータが備えているセキュリティ機能によって、コンピュータ自体、個人情報、およびデータをさまざまなリスクから保護できます。使用する必要があるセキュリティ機能は、コンピュータをどのように使用するかによって決まります。

Windows®オペレーティング システムにより、特定のセキュリティ機能が提供されます。以下の表に、追加のセキュリティ機能の一覧を示します。これらの機能のほとんどは、[Computer Setup]ユーティリティ（以下「[Computer Setup]」と呼びます）で設定できます。

セキュリティの対象	使用するセキュリティ機能
コンピュータの不正な使用	• パスワードまたはスマート カードの使用による電源投入時の認証 • [HP ProtectTools Security Manager]（HP ProtectTools セキュリティ マネージャ）
[Computer Setup]（f10）への不正なアクセス	[Computer Setup]のセットアップ パスワード*
ハードドライブのデータへの不正なアクセス	[Computer Setup]の DriveLock パスワード*
[Computer Setup]（f10）の各種パスワードの不正な再設定	[Computer Setup]の厳重なセキュリティ機能*
オプティカル ドライブ、フロッピー ディスク ドライブ、または内蔵ネットワーク アダプタからの不正な起動	[Computer Setup]のブート オプション機能*
Windows ユーザ アカウントへの不正なアクセス	HP ProtectTools Security Manager
データへの不正なアクセス	• ファイアウォール ソフトウェア • Windows Update • HP ProtectTools Security Manager
[Computer Setup]の設定およびその他のシステム識別情報への不正なアクセス	[Computer Setup]のセットアップ パスワード*

セキュリティの対象	使用するセキュリティ機能
コンピュータの不正な移動	セキュリティ ロック ケーブル用スロット（別売のセキュリティ ロック ケーブルとともに使用）

*[Computer Setup]は、コンピュータの電源投入時または再起動時に f10 キーを押してアクセスするユーティリティであり、Windows が起動する前に機能するユーティリティです。[Computer Setup]の項目間を移動したり項目を選択したりするには、コンピュータのキーを使用する必要があります。

2 パスワードの使用

ほとんどのセキュリティ機能では、パスワードが使用されます。パスワードを設定したときは、そのパスワードを常に書き留めておき、コンピュータから離れた他人の目にふれない安全な場所に保管してください。パスワードに関する以下の考慮事項に注意してください。

- セットアップ パスワード、電源投入時パスワード、および DriveLock パスワードは、[Computer Setup]で設定され、システム BIOS によって管理されます。
- スマート カードの PIN および内蔵セキュリティ パスワードは[HP ProtectTools Security Manager]（HP ProtectTools セキュリティ マネージャ）のパスワードであり、[Computer Setup]で有効に設定することで、通常の[HP ProtectTools]の機能に加えて BIOS パスワードによって保護されます。スマート カードの PIN は対応するスマート カード リーダーとともに、内蔵セキュリティ パスワードはオプションの内蔵セキュリティ チップとともに使用されます。
- Windows パスワードは、Windows オペレーティング システムにのみ設定されます。
- [Computer Setup]で設定したセットアップ パスワードを忘れてしまった場合は、[Computer Setup]にアクセスできなくなります。
- [Computer Setup]で厳重なセキュリティ機能を有効に設定してあり、セットアップ パスワードまたは電源投入時パスワードを忘れてしまった場合は、コンピュータにアクセスできず、永久に使用できなくなります。詳しくは、テクニカル サポートまたは HP 認定のサービス プロバイダにお問い合わせください。
- [Computer Setup]で設定した電源投入時パスワードとセットアップ パスワードの両方を忘れてしまった場合は、コンピュータを起動したりハイバネーションを終了したりできなくなります。詳しくは、テクニカル サポートまたは HP 認定のサービス プロバイダにお問い合わせください。
- [Computer Setup]で設定した DriveLock の user password（ユーザ パスワード）と master password（マスタ パスワード）の両方を忘れてしまうと、これらのパスワードで保護されているハードドライブがロックされたままになり、永久に使用できなくなります。これらのパスワードを両方とも忘れたためにハードドライブを交換する必要が生じた場合、保証期間内でもドライブの交換は有償で承っておりますのでご了承ください。

[Computer Setup]機能と Windows のセキュリティ機能の両方で同じパスワードを使用できます。複数の[Computer Setup]機能で同じパスワードを使用することもできます。

パスワードを作成したり保存したりするときは、以下のヒントを参考にしてください。

- パスワードを作成するときは、プログラムの要件に従う
- パスワードを書き留めておき、コンピュータから離れた他人の目にふれない安全な場所に保管する
- パスワードをコンピュータ上のファイルに保存しない

以下の表によく使用される Windows のパスワードと[Computer Setup]のパスワードの一覧を示し、それぞれの機能を説明します。

Windows でのパスワードの設定

Windows のパスワード	機能
管理者パスワード*	Windows の管理者レベルのアカウントへのアクセスを保護します
ユーザ パスワード*	Windows ユーザ アカウントへのアクセスを保護します
*Windows の管理者パスワードまたは Windows のユーザ パスワードの設定については、**[スタート]**→**[ヘルプとサポート]**の順に選択してください。	

[Computer Setup]でのパスワードの設定

[Computer Setup]のパスワード	機能
セットアップ パスワード	[Computer Setup]へのアクセスを保護します
電源投入時パスワード	コンピュータの起動や再起動、またはハイバネーションの終了時にコンピュータのデータを保護します
DriveLock の master password（マスタ パスワード）	DriveLock によって保護されている内蔵ハードドライブへのアクセスを保護します。また、DriveLock による保護の解除に使用します。このパスワードは DriveLock を有効にする操作の過程で設定します
DriveLock の user password（ユーザ パスワード）	DriveLock によって保護されている内蔵ハードドライブへのアクセスを保護します。DriveLock を有効にする操作の過程で設定します
スマート カードの PIN	スマート カードおよび Java™ Card のコンテンツへのアクセスを保護し、スマート カード、Java Card、およびスマート カード リーダが使用されているときにコンピュータのアクセスを保護します
TPM 内蔵セキュリティ パスワード	BIOS パスワードとして有効にすると、コンピュータの起動や再起動、またはハイバネーションの終了時にコンピュータのデータを保護します このパスワードを使用するには、オプションの内蔵セキュリティ チップでこのセキュリティ機能がサポートされている必要があります

セットアップ パスワード

[Computer Setup]のセットアップ パスワードは、[Computer Setup]内の各種設定とシステム識別情報を保護します。このパスワードを設定した場合は、[Computer Setup]にアクセスして変更を行うときにパスワードを入力する必要があります。

セットアップ パスワードには以下のような特徴があります。

- [Computer Setup]のセットアップ パスワードと Windows の管理者パスワードには同じ文字列を使用できますが、互いに代替できるものではありません。
- パスワードは、設定、入力、変更または削除する際に画面に表示されません。
- パスワードを入力するときは、設定したときと同じキーを使う必要があります。たとえば、ファンクション キーの下にある数字キーを使ってセットアップ パスワードを設定した場合、その後内蔵テンキーを使って入力しても同じ文字として認識されません。
- 32 文字以内の半角英数字の組み合わせで、大文字と小文字は区別されません。

セットアップ パスワードの管理

セットアップ パスワードは、[Computer Setup]で設定、変更、および削除できます。

このパスワードを管理、設定、変更、および削除するには、以下の手順で操作します。

1. コンピュータを起動または再起動し、画面の左下隅に[F10=ROM Based Setup]メッセージが表示されている間に f10 キーを押して、[Computer Setup]を起動します。
2. 矢印キーを使用して**[Security]**（セキュリティ設定）→**[Setup password]**（セットアップ パスワード）の順に選択し、enter キーを押します。
   - セットアップ パスワードを設定するには、**[New password]**（新しいパスワード）フィールドと**[Verify new password]**（新しいパスワードの確認入力）フィールドにパスワードを入力して、f10 キーを押します。
   - セットアップ パスワードを変更するには、**[Old password]**（現在のパスワード）フィールドに現在のパスワードを、**[New password]**フィールドと**[Verify new password]**フィールドに新しいパスワードを入力して、f10 キーを押します。
   - セットアップ パスワードを削除するには、**[Old password]**フィールドに現在のパスワードを入力して、f10 キーを押します。
3. 設定内容を保存するには、矢印キーを使用して**[File]**（ファイル）→**[Save changes and exit]**（変更を保存して終了）の順に選択してから、画面の説明に沿って操作します。

選択または設定した内容は、コンピュータの再起動時に有効になります。

セットアップ パスワードの入力

セットアップ パスワードの入力画面が表示されたらセットアップ パスワードを設定したときと同じ種類のキーを使用して入力し、enter キーを押します。3 回続けて間違えて入力した場合は、コンピュータを再起動し、入力しなおしてください。

電源投入時パスワード

[Computer Setup]の電源投入時パスワードは、コンピュータの不正使用を防止します。このパスワードを設定した場合は、コンピュータの電源を入れたときに毎回パスワードを入力する必要があります。

電源投入時パスワードには以下のような特徴があります。

- パスワードは、設定、入力、変更または削除する際に画面に表示されません。
- パスワードを入力するときは、設定したときと同じキーを使う必要があります。たとえば、ファンクション キーの下にある数字キーを使って電源投入時パスワードを設定した場合、その後内蔵テンキーを使って入力しても同じ文字として認識されません。
- 32 文字以内の半角英数字の組み合わせで、大文字と小文字は区別されません。

電源投入時パスワードの管理

[Computer Setup]を使用して、電源投入時パスワードを設定、変更、および削除できます。

このパスワードを管理、設定、変更、および削除するには、以下の手順で操作します。

1. コンピュータを起動または再起動し、画面の左下隅に[F10=ROM Based Setup]メッセージが表示されている間に f10 キーを押して、[Computer Setup]を起動します。
2. 矢印キーを使用して**[Security]**（セキュリティ設定）→**[Power-On password]**（電源投入時パスワード）の順に選択し、enter キーを押します。
   - 電源投入時パスワードを設定するには、**[New password]**（新しいパスワード）フィールドと**[Verify new password]**（新しいパスワードの確認入力）フィールドにパスワードを入力して、f10 キーを押します。
   - 電源投入時パスワードを変更するには、**[Old password]**（現在のパスワード）フィールドに現在のパスワードを、**[New password]**フィールドと**[Verify new password]**フィールドに新しいパスワードを入力して、f10 キーを押します。
   - 電源投入時パスワードを削除するには、**[Old password]**フィールドに現在のパスワードを入力して、f10 キーを押します。
3. 設定内容を保存するには、矢印キーを使用して**[File]**（ファイル）→**[Save changes and exit]**（変更を保存して終了）の順に選択してから、画面の説明に沿って操作します。

選択または設定した内容は、コンピュータの再起動時に有効になります。

電源投入時パスワードの入力

電源投入時パスワードの入力画面が表示されたら、電源投入時パスワードを設定したときと同じ種類のキーを使用して入力し、enter キーを押します。3 回続けて間違えて入力した場合は、コンピュータの電源を切ってから再び起動し、入力しなおしてください。

再起動時の電源投入時パスワードの入力要求

電源投入時パスワードは、コンピュータの電源を入れたときだけでなく、コンピュータを再起動するたびに入力を要求するように設定できます。

[Computer Setup]でこの機能を有効または無効にするには、以下の手順で操作します。

1. コンピュータを起動または再起動し、画面の左下隅に[F10=ROM Based Setup]メッセージが表示されている間に f10 キーを押して、[Computer Setup]を起動します。
2. 矢印キーを使用して**[Security]**（セキュリティ設定）→**[Password options]**（パスワード オプション）の順に選択し、enter キーを押します。
3. 矢印キーを使用して**[Require password on restart]**（再起動時にパスワードを要求する）フィールドの**[Enable]**（有効）または**[Disable]**（無効）を選択し、f10 キーを押します。
4. 設定内容を保存するには、矢印キーを使用して**[File]**（ファイル）→**[Save changes and exit]**（変更を保存して終了）の順に選択してから、画面の説明に沿って操作します。

[Computer Setup]の DriveLock（ドライブロック）の使用

△ **注意：** DriveLock で保護されているハードドライブが永久に使用できなくなることを防ぐため、DriveLock の user password（ユーザ パスワード）と master password（マスタ パスワード）を、紙などに書いて他人の目にふれない安全な場所に保管しておいてください。DriveLock パスワードを両方とも忘れてしまうと、これらのパスワードで保護されているハードドライブがロックされたままになり、永久に使用できなくなります。なお、master password と user password を両方とも忘れたためにハードドライブを交換する必要が生じた場合、保証期間内でもドライブの交換は有償で承っておりますのでご了承ください。

DriveLock でのプロテクトによって、ハードドライブのデータへの不正なアクセスを防止できます。DriveLock によるプロテクトはコンピュータ本体のベイに取り付けられているハードドライブにのみ設定できます。いったん DriveLock によるプロテクトを設定すると、ドライブにアクセスするときにパスワードの入力が必要になります。DriveLock のパスワードでドライブにアクセスするには、ドライブを別売のドッキング デバイスや外付けマルチベイではなく、コンピュータに装着しておく必要があります。

DriveLock によるプロテクトをコンピュータの内蔵ハードドライブに設定するには、[Computer Setup] で user password および master password を設定しておく必要があります。DriveLock によるプロテクトを設定するときは、以下の点に注意してください。

- いったん DriveLock によるプロテクトを設定すると、user password または master password のどちらかを入力することでのみ、プロテクトされているハードドライブにアクセスできるようになります。
- user password は、通常システム管理者ではなく実際にハードドライブを使用するユーザが設定する必要があります。master password は、システム管理者または実際にハードドライブを使用するユーザが設定できます。
- user password と master password は、同じであってもかまいません。
- DriveLock によるドライブのプロテクトを解除しないと、user password や master password を削除できません。DriveLock によるハードドライブのプロテクトを解除するには、master password が必要です。

注記： 電源投入時パスワード（Power-on password）と DriveLock パスワードの両方に同じパスワードを使用している場合、電源投入時パスワードと DriveLock の user password の両方の入力ではなく、電源投入時パスワードの入力のみを要求されます。

DriveLock パスワードの設定

[Computer Setup]で DriveLock の設定値にアクセスするには、以下の手順で操作します。

1. コンピュータを起動または再起動し、画面の左下隅に[F10=ROM Based Setup]メッセージが表示されている間に f10 キーを押して、[Computer Setup]を起動します。
2. 矢印キーを使用して**[Security]**（セキュリティ設定）→**[DriveLock passwords]**（DriveLock パスワード）の順に選択し、enter キーを押します。
3. プロテクトするハードドライブが搭載されているベイを選択して、f10 キーを押します。
4. 矢印キーを使用して**[Protection]**（保護）フィールドの**[Enable]**（有効）を選択し、f10 キーを押します。
5. 警告メッセージが表示されます。操作を続ける場合は、f10 キーを押します。
6. user password（ユーザ パスワード）を**[New password]**（新しいパスワード）フィールドと**[Verify new password]**（新しいパスワードの確認入力）フィールドに入力して、f10 キーを押します。
7. master password（マスタ パスワード）を**[New password]**フィールドと**[Verify new password]**フィールドに入力して、f10 キーを押します。
8. 選択したドライブが DriveLock によって保護されているかを確認するには、確認フィールドに「DriveLock」と入力し、f10 キーを押します。
9. 矢印キーを使用して**[Esc]**（終了）を選択し、DriveLock 設定を終了します。
10. 設定内容を保存するには、矢印キーを使用して**[File]**（ファイル）→**[Save changes and exit]**（変更を保存して終了）の順に選択してから、画面の説明に沿って操作します。

選択または設定した内容は、コンピュータの再起動時に有効になります。

DriveLock パスワードの入力

ハードドライブが、別売のドッキング デバイスや外付けマルチベイではなくコンピュータ本体のハードドライブ ベイに装着されていることを確認します。

[DriveLock Password]（DriveLock パスワード）画面が表示されたら、パスワードを設定したときと同じ種類のキーを使用して user password（ユーザ パスワード）または master password（マスタ パスワード）を入力し、enter キーを押します。

パスワードを 2 回続けて間違えて入力した場合は、コンピュータの電源を切ってから再び起動し、入力しなおしてください。

DriveLock パスワードの変更

[Computer Setup]で DriveLock パスワードを変更するには、以下の手順で操作します。

1. コンピュータを起動または再起動し、画面の左下隅に[F10=ROM Based Setup]メッセージが表示されている間に f10 キーを押して、[Computer Setup]を起動します。
2. 矢印キーを使用して**[Security]**（セキュリティ設定）→**[DriveLock passwords]**（DriveLock パスワード）の順に選択し、enter キーを押します。
3. 矢印キーを使用して内蔵ハードドライブの場所を選択し、f10 キーを押します。
4. 矢印キーを使用して、変更するパスワードのフィールドを選択します。**[Old password]**（現在のパスワード）フィールドに現在のパスワードを入力してから、**[New password]**（新しいパスワード）フィールドと**[Verify new password]**（新しいパスワードの確認）フィールドに新しいパスワードを入力して、f10 キーを押します。
5. 設定内容を保存するには、矢印キーを使用して**[File]**（ファイル）→**[Save changes and exit]**（変更を保存して終了）の順に選択してから、画面の説明に沿って操作します。

選択または設定した内容は、コンピュータの再起動時に有効になります。

DriveLock 保護の解除

[Computer Setup]で DriveLock による保護を解除するには、以下の手順で操作します。

1. コンピュータを起動または再起動し、画面の左下隅に[F10=ROM Based Setup]メッセージが表示されている間に f10 キーを押して、[Computer Setup]を起動します。
2. 矢印キーを使用して**[Security]**（セキュリティ設定）→**[DriveLock passwords]**（DriveLock パスワード）の順に選択し、enter キーを押します。
3. 矢印キーを使用して内蔵ハードドライブの場所を選択し、f10 キーを押します。
4. 矢印キーを使用して**[Protection]**（保護）フィールドの**[Disable]**（無効）を選択し、f10 キーを押します。
5. **[Old password]**（現在のパスワード）フィールドに master password（マスタ パスワード）を入力し、f10 キーを押します。
6. 設定内容を保存するには、矢印キーを使用して**[File]**（ファイル）→**[Save changes and exit]**（変更を保存して終了）の順に選択してから、画面の説明に沿って操作します。

選択または設定した内容は、コンピュータの再起動時に有効になります。

3 [Computer Setup]のセキュリティ機能の使用

システム デバイスのセキュリティ保護

[Computer Setup]の[Boot options]（ブート オプション）メニューまたは[Port options]（ポート オプション）メニューから、システム デバイスを有効または無効にできます。

[Computer Setup]でシステム デバイスを無効または再び有効にするには、以下の手順で操作します。

1. コンピュータを起動または再起動し、画面の左下隅に[F10=ROM Based Setup]メッセージが表示されている間に f10 キーを押して、[Computer Setup]を起動します。
2. 矢印キーを使用して**[System Configuration]**（システム コンフィギュレーション）→**[Boot options]**または**[System Configuration]**→**[Port options]**の順に選択します。次に、enter キーを押してから、矢印キーを使用して設定を選択します。
3. 設定を確定するには、f10 キーを押します。
4. 設定内容を保存するには、矢印キーを使用して**[File]**（ファイル）→**[Save changes and exit]**（変更を保存して終了）の順に選択してから、画面の説明に沿って操作します。

選択または設定した内容は、コンピュータの再起動時に有効になります。

[Computer Setup]の厳重なセキュリティの使用

△ **注意：** コンピュータが永久に使用不能になる事態を回避するために、設定されたセットアップ パスワード、電源投入時パスワード、またはスマート カード PIN を記録して、コンピュータとは別の他人の目にふれない安全な場所に保管しておいてください。これらのパスワードまたは PIN がなければ、コンピュータのロックを解除することはできません。

厳重なセキュリティ機能を使用すると、システムへのアクセスを許可する前に、設定済みのセットアップ パスワード、電源投入時パスワード、またはスマート カード PIN を使用してユーザ認証を実行することにより、電源投入時のセキュリティを強化できます。

厳重なセキュリティの設定

[Computer Setup]で厳重なセキュリティを有効にするには、以下の手順で操作します。

1. コンピュータを起動または再起動し、画面の左下隅に[F10=ROM Based Setup]メッセージが表示されている間に f10 キーを押して、[Computer Setup]を起動します。
2. 矢印キーを使用して**[Security]**（セキュリティ設定）→**[Password options]**（パスワード オプション）の順に選択し、enter キーを押します。
3. 矢印キーを使用して、**[Stringent security]**（厳重なセキュリティ）フィールドで**[Enable]**（有効）を選択します。
4. 警告メッセージが表示されます。続行するには、f10 キーを押します。
5. コンピュータの電源を入れるたびにこの機能を有効にするには、f10 キーを押します。
6. 設定内容を保存するには、矢印キーを使用して**[File]**（ファイル）→**[Save changes and exit]**（変更を保存して終了）の順に選択してから、画面の説明に沿って操作します。

選択または設定した内容は、コンピュータの再起動時に有効になります。

厳重なセキュリティによるプロテクトの解除

[Computer Setup]で厳重なセキュリティによるプロテクトを解除するには、以下の手順で操作します。

1. コンピュータを起動または再起動し、画面の左下隅に[F10=ROM Based Setup]メッセージが表示されている間に f10 キーを押して、[Computer Setup]を起動します。
2. 矢印キーを使用して**[Security]**（セキュリティ設定）→**[Password options]**（パスワード オプション）の順に選択し、enter キーを押します。
3. 矢印キーを使用して**[Stringent security]**（厳重なセキュリティ）フィールドで**[Disable]**（無効）を選択し、f10 キーを押します。
4. 設定内容を保存するには、矢印キーを使用して**[File]**（ファイル）→**[Save changes and exit]**（変更を保存して終了）の順に選択してから、画面の説明に沿って操作します。

選択または設定した内容は、コンピュータの再起動時に有効になります。

[Computer Setup]のシステム情報の表示

[Computer Setup]の[System Information]（システム情報）機能は、以下の 2 種類のシステム情報を表示できます。

- コンピュータのモデルおよびバッテリについての識別情報
- プロセッサ、キャッシュ、メモリ、ROM、ビデオとキーボード コントローラのバージョンに関する仕様情報

[Computer Setup]でこのシステム情報全般を表示するには、以下の手順で操作します。

1. コンピュータを起動または再起動し、画面の左下隅に[F10=ROM Based Setup]メッセージが表示されている間に f10 キーを押して、[Computer Setup]を起動します。
2. 矢印キーを使用して**[File]**（ファイル）→**[System Information]**の順に選択し、enter キーを押します。

注記： この情報への不正なアクセスを防ぐには、[Computer Setup]でセットアップ パスワードを作成する必要があります。

[Computer Setup]のシステム ID の使用

[Computer Setup]の[System ID]（システム ID）機能では、コンピュータのアセット タグおよびオーナーシップ タグを表示または入力できます。

注記： この情報への不正なアクセスを防ぐには、[Computer Setup]でセットアップ パスワードを作成する必要があります。

[Computer Setup]でこの機能を管理するには、以下の手順で操作します。

1. コンピュータを起動または再起動し、画面の左下隅に[F10=ROM Based Setup]メッセージが表示されている間に f10 キーを押して、[Computer Setup]を起動します。
2. 矢印キーを使用して**[Security]**（セキュリティ設定）→**[System ID]**の順に選択し、enter キーを押します。
3. アセット タグの情報を入力するには、矢印キーを使用して**[Asset Tracking Number]**（アセット タグ）フィールドまたは**[Ownership Tag]**（オーナーシップ タグ）フィールドを強調表示してから、情報を入力します。
4. 設定が終了したら、f10 キーを押します。
5. 設定内容を保存するには、矢印キーを使用して**[File]**（ファイル）→**[Save changes and exit]**（変更を保存して終了）の順に選択してから、画面の説明に沿って操作します。

選択または設定した内容は、コンピュータの再起動時に有効になります。

4 ウィルス対策ソフトウェアの使用

コンピュータで電子メール、ネットワーク、またはインターネットにアクセスする場合、コンピュータがコンピュータ ウィルスの危険にさらされます。コンピュータ ウィルスに感染すると、オペレーティング システム、プログラム、ユーティリティなどが使用できなくなったり、正常に動作しなくなったりすることがあります。

ウィルス対策ソフトウェアを使用すると、既知のウィルスを検出および駆除したり、多くの場合はウィルスの被害にあった箇所を修復したりできます。新しく発見されたウィルスからコンピュータを保護するには、ウィルス対策ソフトウェアを最新の状態に保つ必要があります。

お使いのコンピュータには、[McAfee Total Protection]ウィルス対策ソフトウェアがプリインストールされています。インストールされているソフトウェアにアクセスするには、**[スタート]**→**[すべてのプログラム]**→**[McAfee]**→**[Managing Services]**（管理サービス）→**[Total Protection]**（トータル プロテクション）の順に選択します。

コンピュータ ウィルスについてさらに詳しく調べるには、[ヘルプとサポート]の[検索]テキスト フィールドに「ウィルス」と入力してください。

5　ファイアウォール ソフトウェアの使用

コンピュータで電子メールやネットワークを使用したりインターネットにアクセスしたりする場合、使用者や使用しているコンピュータ、使用者の個人用ファイル、および使用者に関する情報を、第三者が不正に取得してしまう可能性があります。プライバシを保護するため、コンピュータにプリインストールされているファイアウォール ソフトウェアを使用してください。

ファイアウォール機能によって、ネットワーク接続時の操作に関するログおよびレポートが記録され、コンピュータでの送受信の流れが自動的に監視されます。詳しくは、ソフトウェアの製造元の説明書を参照してください。

注記：　特定の状況下では、ファイアウォールがインターネット ゲームへのアクセスをブロックしたり、ネットワーク上のプリンタやファイルの共有に干渉したり、許可されている電子メールの添付ファイルをブロックしたりすることがあります。問題を一時的に解決するには、ファイアウォールを無効にして目的のタスクを実行した後で、ファイアウォールを再度有効にします。問題を永久に解決するには、ファイアウォールを再設定します。

6 緊急セキュリティ アップデートのインストール

△ **注意：** Microsoft 社は、緊急セキュリティ アップデートに関する通知を配信しています。お使いのコンピュータをセキュリティの侵害やコンピュータ ウィルスから保護するため、通知があった場合はすぐに Microsoft 社からのオンライン緊急アップデートをインストールしてください。

オペレーティング システムやその他のソフトウェアに対するアップデートが、コンピュータの工場出荷後にリリースされている可能性があります。すべての使用可能なアップデートが確実にコンピュータにインストールされているようにするには、以下の操作を行います。

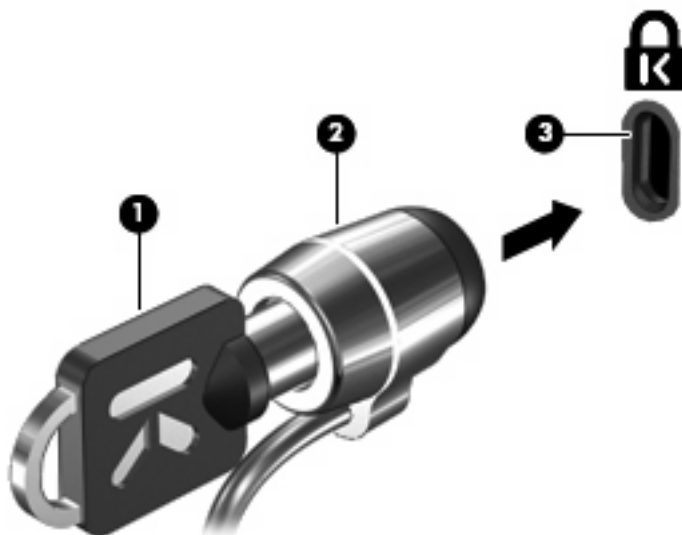
- Windows Update を毎月実行して、Microsoft 社から最新のソフトウェアをインストールします。
- アップデートがリリースされるたびに、Microsoft 社の Web サイトおよび**[ヘルプとサポート]**のアップデート リンクから入手します。

7 [HP ProtectTools Security Manager]（HP ProtectTools セキュリティ マネージャ）の使用（一部のモデルのみ）

一部のモデルのコンピュータでは、[HP ProtectTools Security Manager]ソフトウェアがプリインストールされています。このソフトウェアは、Windows の**[コントロール パネル]**からアクセスすることができます。このソフトウェアが提供するセキュリティ機能は、コンピュータ本体、ネットワーク、および重要なデータを不正なアクセスから保護するために役立ちます。詳しくは、[HP ProtectTools]のヘルプを参照してください。

8 セキュリティ ロック ケーブルの取り付け

注記： セキュリティ ロック ケーブルに抑止効果はありますが、コンピュータの誤った取り扱いや盗難を完全に防ぐものではありません。

1. セキュリティ ロック ケーブルを固定された物体に巻きつけます。
2. 鍵（**1**）をケーブル ロック（**2**）に差し込みます。
3. ケーブル ロックをコンピュータのセキュリティ ロック ケーブル用スロット（**3**）に差し込み、鍵を回転させてケーブル ロックを固定します。

注記： お使いのコンピュータの外観は、図と異なる場合があります。セキュリティ ロック ケーブル用スロットの位置は、コンピュータのモデルによって異なります。

索引